upwind

Cloud Security Assessment Report

Table of Contents

1. Objective

Purpose

Upwind's free cloud security assesment is a simple tool for rapidly identifying key risks, attacks paths, and critical posture findings in your cloud environment. The initial setup takes around 5 minutes, and can be done individually or with the help of an Upwind technical expert. In this document, we give a brief outline of what to expect from the cloud security assessment including time needed, expected findings, and setup needs.

Goals

- **Business Outcomes:** Present results in terms of tangible security
- **Ease of Deployment:** Showcase Upwind's low-friction, cloud-native setup
- **24 Hour Deliverables:** Define security insights deliverable within the first 24 hours of the assessment

2. Assessment Scope

Deployment Model:

- **(Basic) Agentless CSPM:** Cloud accounts scanned for misconfigurations, public exposure, and vulnerabilities
- **(Advanced) KSPM + Runtime (Phase 2):** Kubernetes misconfiguration and runtime exploit analysis.

Cloud Environments Covered:

- AWS, Azure, GCP (based on your capabilities).

Initial Assessment Duration:

- 12-24 hours

Assessment Deliverables:

- **Security Findings:** Actionable security insights.
- **Compliance Posture:** Against benchmarks (e.g., CIS).
- **Risk Prioritization:** Highlight critical vulnerabilities with potential exploit paths.

3. Security Insights and Deliverables

A) Cloud Security Posture Assessment (CSPM) – Basic Phase

Key Findings

- **Misconfigurations & Exposure:**
  - Identify publicly exposed assets with vulnerabilities.
  - Detect insecure S3 buckets and cloud storage permissions.
- **Critical Vulnerabilities:**
  - List CVEs with known exploits.
- **Data Insights:**
  - Detect generative AI platforms being used.
  - Identify suspicious CloudTrail activity.
- **Identity Insights:**
  - Enforcement of Principal of Least Privilege
  - Identifying accounts that have not been used in 180 days+
  - Identifying accounts with permissions that have never been used
  - Identifying System Accounts with unused permissions

Compliance Posture

- CIS Benchmark adherence summary.
- Compliance heatmap (if applicable).

24-Hour Deliverable Example:

- List of critical vulnerabilities with public exploits.
- List of exposed S3 buckets.
- Summary of suspicious CloudTrail activity.
- Identity insights to remediate immediately.

3. Security Insights and Deliverables

B) Kubernetes Security Posture Assessment (KSPM) – Advanced Phase

Key Findings

- **K8s Misconfigurations:**
  - Identify exposed clusters/nodes
  - Highlight excessive privileges or misconfigurations
- **Runtime Threats:**
  - Detect actively exploited vulnerabilities
  - Identify suspicious runtime behavior or dirty traffic
- **Runtime Exploit Funnel:**
  - Prioritize vulnerabilities based on exploitability
- **API Catalog:**
  - Discover exposed or misconfigured APIs

Advanced Deliverable Example:

- List of K8s misconfigurations.
- Runtime vulnerabilities with real exploit attempts.
- API catalog summary.

4. Compliance and Risk Prioritization

Frameworks Evaluated:

- CIS Benchmarks (CSPM).
- PCI, HIPAA, or NIST (optional extensions).

Risk Severity Scoring:

- Categorized by critical, high, medium, and low severity.

Attack Path Analysis:

- Map attack paths from misconfigurations and vulnerabilities to potential exploitation.

5. Next Steps and Recommendations

Immediate Remediation Suggestions:

- Actions to reduce public exposure.
- Patching guidance for critical CVEs.
- Misconfiguration fixes.

Ongoing Monitoring:

- Recommend continuous runtime and posture monitoring.

Final Output

This document provides a standardized Cloud Security Assessment format that clearly defines scope, deliverables, and actionable outcomes.

For an example of Cloud Security Assessment results and typical findings please visit the following link.

Example Cloud Security Assessment